SBIR TOPIC N99-34 PHASE II SUPPORT

Wolfgang Baer, Research Assistant Professor Department of Computer Science Sponsor: Office of Naval Research

OBJECTIVE: Monitor the development of an intrinsic earth surface classification system for application toward a one meter resolution earth surface standard model.

DoD KEY TECHNOLOGY AREAS: Human Systems Interface

KEYWORDS: Simulation, Battlefield Visualization, High Resolution Terrain, Remote Sensing

HIGH RESOLUTION TERRAIN SYSTEMS DEVELOPMENT AND DATA SUPPORT

Wolfgang Baer, Research Assistant Professor Department of Computer Science Sponsor: U.S. Army Experimentation Command

OBJECTIVE: The scientific objective of this research is to provide system and software development support for high-resolution database creation, visualization, analysis and integration into operational systems. Tasks include the development of prototype systems and software capable of displaying the high-resolution (1-meter) terrain, and enhancement of after action review capabilities using such products as low cost PC based workstations. Support is also provided for the initialization and construction of sample databases and the porting and testing of existing tools to low cost networked commodity based computer systems.

DoD KEY TECHNOLOGY AREAS: Human Systems Interface

KEYWORDS: Simulation, Battlefield Visualization, High Resolution, Terrain

MICRO TERRAIN TOOLS DEVELOPMENT SUPPORT

Wolfgang Baer Research Assistant Professor Department of Computer Science Sponsor: U.S. Army Operational Test Command

OBJECTIVE: Terrain Database Generation Tool Development.

SUMMARY: Provides a tool to build a resolution 1-meter terrain database. The database is initialized using standard elevation models (DTED). It then integrates higher resolution ortho-rectified photo imagery and higher accuracy elevation data from a terrain patch of interest. Finally the tool will recognize terrain feature classes such as trees, bushes, rocks, etc. and perform a 3-D model fit. The tools also provide for interactive editing of the terrain database in order to allow cosmetic and high fidelity corrections.

A Sunview version of the tool was developed for terrain generation at Ft. Hunter Liggett. The tool is now being rewritten for operation in COTS PC hardware under Windows 2000.

The tool will be delivered in FY 2001 in order to support a 64x64 km database construction at Fort Hood, Texas.

PRESENTATION:

Grewe, L.L., Rowe, N., and Baer, W., "AERICOMP: An Aerial Photo Comparison System," SPIE's AeroSense: Signal Processing, Sensor Fusion, and Target Recognition, San Jose, CA, April 2000.

DoD KEY TECHNOLOGY AREAS: Modeling and Simulation

KEYWORDS: Terrain Modeling, Pattern Recognition, Geographic Tomography

BATTLEFIELD DATA PROCESSING COURSE DEVELOPMENT

Wolfgang Baer, ResearchAssistant Professor Department of Computer Science Sponsor: Officer of Naval Research

OBJECTIVE: Develop a Course and Research Capability to Support Integration of Virtual Reality and Battlefield Sensing.

SUMMARY: Closing the loop between battlefield sensors and military computer systems in a timely and accurate manner is one of the key requirements for information superiority in 21'st century military operations. Future command centers will integrate virtual reality technologies with real-time battlefield sensing systems to support battlefield decisions and data product generation. It is imperative that the future commanders understand the concepts, limits, and capacities of such systems.

The course we plan to develop focuses on the generation of virtual environment databases. Emphasis will be on the techniques, data sources, and active research areas, which produce realistic representations of geographic areas of military interest.

THESIS DIRECTED:

Hunter, J.B. and Grossman, H., "Network Track; Universal Traffic Network," Masters Thesis, Naval Postgraduate School, September 2000.

DoD KEY TECHNOLOGY AREAS: Modeling and Simulation

KEYWORDS: Sensors, Signal Processing, Communications, Terrain Modeling

TRACER/FCS HIGH RESOLUTION TERRAIN STUDY

Wolfgang Baer, Research Assistant Professor Department of Computer Science Sponsor: U.S. Army TRADOC Analysis Command-Monterey

OBJECTIVE: Develop mission scenarios and measure the delectability vs. mission effectiveness of newly proposed scout vehicle designs using the high resolution one meter battlefield terrain simulators.

SUMMARY: TRADOC has been tasked to conduct a TRACER/FSCS Combined Analysis. The objective of this analysis is to determine the most cost effective TRACER/FSCS ground scout system to replace the Bradley Calvary Fighting Vehicle (CFV) and the High Mobility Multi-Purpose Wheeled Vehicle (HMMWV) used by U.S. Forces, and the Combat Vehicle Reconnaissance Tracked (CVR (T) used by UK Forces.

The purpose of this work is two fold: (1) Define the scenarios, measurements, and software controls and algorithms required to conduct a meaningful analysis of the TRACER/FSCS ground scout system; (2) Develop the support software and execute the analysis if deemed feasible and cost effective.

PUBLICATIONS:

Baer, W., Illingworth, J., Kemple, W., and Mansager, B., "Weapons Design Analysis Using One Meter Terrain Resolution Battlefield Simulators-I," *Proceedings of the 2000 Summer Computer Simulation Conference*, Bill Waite and Abe Nisanci, eds., Vancouver, BC, 16-20 July 2000.

Illingworth, J., Baer, W., and Mansager, B., "Weapons Design Analysis Using One Meter Terrain Resolution Battlefield Simulators-II," 2000 Fall Simulation Interoperability Workshop, Workshop Paper 00F-SIW-118, 17-22 September 2000, Orlando, FL.

DoD KEY TECHNOLOGY AREAS: Modeling and Simulation

KEYWORDS: Line-of-Sight, Terrain Modeling, Weapons Design Simulation

SISO INTRINSIC EARTH SURFACE MATERIAL CLASSIFIER SYSTEM PHASE II

Wolfgang Baer, Research Assistant Professor Department of Computer Science Sponsor: Office of Naval Research

OBJECTIVE: Build the infrastructure for the construction of such an earth surface material database at one-meter resolution.

SUMMARY: The Simulation Interoperability Standards Organization (SISO) Intrinsic Earth Surface Material Classifier System project will develop the definition of a Standard Surface Material Code (SSMC). To a modeling and simulation program, such a code acts like a pointer to a list of intrinsic earth surface material parameter values that define the physical and radiometric properties of the surface over a broad wavelength range. This information will reside in the Surface Materials Standards list - RESOLVE (Radiometric Earth Surface Observable for Land Visualization Events), which includes materials based on the global abundance of naturally-occurring, man-made, and non-realistic materials, their significance (e.g. importance) to a user community, and availability of spectral data sources to support extraction of intrinsic surface properties. The standard will also include reversible surface rendering and atmospheric propagation equations to allow a traceable connection between measurement and database content. Tools for extracting intrinsic properties of material from remotely required data are basically nonexistent and the suites of surface rendering tools currently available are limited in scope; in other words, they cover an abbreviated wavelength range or include only a limited set of material types. The goal of our effort is to build the infrastructure for the construction of such an earth surface material database at 1 meter resolution.

PUBLICATION:

Baer, W., Petroy, S., Shepard, M., Jacobs, E., Cornette, B., and Sunshine, J., "Toward Standard Rendering Equation For Intrinsic Earth Surface Classification," 2000 Spring Simulation Interoperability Workshop, Workshop Paper 00S-SIW-70, 26-31 March 2000, IST, Orlando, FL.

DoD KEY TECHNOLOGY AREAS: Modeling and Simulation

KEYWORDS: Remote Sensing, Terrain Modeling, BDRF

AUTOMATION SUPPORT FOR SOFTWARE EVOLUTION

Valdis Berzins, Professor Department of Computer Science Sponsor: U. S. Army Research Office

OBJECTIVE: To design a system for automating the configuration management needed to keep track of the evolution of a software prototype.

SUMMARY: The objective of the research is to design a system for automating the configuration management needed to keep track of the evolution of a software prototype during a typical application of the evolutionary software prototyping method supported by CAPS. The Computer Aided Prototyping

System (CAPS) is an integrated software development environment aimed at rapidly prototyping hard realtime embedded software systems, such as missile guidance systems, space shuttle avionics systems, robots, automated factories, telecommunications systems, computer-controlled vehicles, and computer-controlled consumer appliances such as microwave ovens and sewing machines.

We developed an integrated set of formal models and methods to provide decision support and partial automation for software evolution. The mathematical models capture the attributes of and dependencies between versions of software components, as well as the analysis and design activities that produce them. These models support computer-aided planning, cost estimation, automated configuration management, automated team coordination, automated project scheduling, automated project status monitoring and risk assessments. They provide the formalism for algorithms to automatically manage design information, design rationale, human resources, and plans.

PUBLICATIONS:

Berzins, V., Shing, M., Luqi, Saluto, M., and Williams, J., "Architectural Re-Engineering of Janus Using Object Modeling and Rapid Prototyping," *Journal of Design Automation for Embedded Systems*, 5(3/4), August 2000, pp.251-263.

Berzins, V., Shing, M., Luqi, Saluto, M., and Williams, J., "Object-Oriented Modular Architecture for Ground Combat Simulation," *Proceedings of the 2000 Command and Control Research and Technology Symposium*, Naval Postgraduate School, Monterey, CA, 26-28 June 2000.

Berzins, V., "Light Weight Inference for Automation Efficiency," submitted to *Science of Computer Programming*.

Harn, M., Berzins, V., and Luqi, "A Formal Model for Software Evolution," *Proceedings of the 3rd International Conference on Computational Intelligence and Multimedia Applications*, New Delhi, India, 23-26 September 1999.

Harn, M., Berzins, V., and Luqi, "Software Evolution Process via a Relational Hypergraph Model," *Proceedings of the IEEE/IEEJ/JSAI International Conference on Intelligent Transportation Systems*, Tokyo, Japan, 5-8 October 1999.

Zhang, D. and Luqi, "Approximate Declarative Semantics for Rule Base Anomalies," *Knowledge-Based Systems*, Vol.12, No.7, November 1999, pp.341-353.

Nogueira, J., Luqi, and Berzins, V., "Risk Assessment in Software Requirement Engineering," *Proceedings of the 5th World Conference on Integrated Design & Process Technology*, Dallas, TX, 4-8 June 2000.

Nogueira, J., Jones, C., and Luqi, "Surfing the Edge of Chaos: Applications to Software Engineering," *Proceedings of the 2000 Command and Control Research and Technology Symposium*, Monterey, CA, 26-28 June 2000.

Nogueira, J., Luqi, Berzins, V., and Nada, N., "A Formal Risk Assessment Model for Software Evolution," *Proceedings of 2nd International Workshop on Economics-Driven Software Engineering Research (EDSER-2) of the 22nd International Conference on Software Engineering (ICSE2000)*, Limerick, Ireland, 4-10 June 2000.

Nogueira, J., Luqi and Bhattacharya, S., "A Risk Assessment Model for Software Prototyping Projects," *Proceedings of the11th IEEE International Workshop on Rapid System Prototyping (RSP2000)*, Paris, France, 21-23 June 2000.

Nada, N., Luqi, Rine, D., and Jaber, K., "Product Line Stakeholder Viewpoint and Validation Models," *Proceedings of the Workshop on Software Product Lines: Economics, Architectures, and Implications of the 22nd International Conference on Software Engineering (ICSE2000)*, Limerick, Ireland, 4-11 June 2000.

- Nada, N., Luqi, Rine, D., and Damiani, E., "A Knowledge-Based System for Software Reuse Technology Practices," *Proceedings of the Third International Workshop on Intelligent Software Engineering (WISE3) of the 22nd International Conference on Software Engineering (ICSE2000)*, Limerick, Ireland, 4-11 June 2000.
- Nada, N., Luqi, Rine, D., and Damiani, E., "A Knowledge-Based Adaptive Distance Learning System for Software Reuse Technology," *Proceedings of the Twelfth International Conference on Software Engineering and Knowledge Engineering (SEKE2000)*, Chicago, IL, 6-8 July 2000.
- Luqi, Berzins, V., Shing, M., Nada, N., and Eagle, C., "Computer Aided Prototyping System (CAPS) for Heterogeneous Systems Development and Integration," *Proceedings of the 2000 Command and Control Research and Technology Symposium*, Naval Postgraduate School, Monterey, CA, 26-28 June 2000.
- Luqi, V. Berzins, M. Shing, R. Riehle and J. Nogueira, "Evolutionary Computer Aided Prototyping System (CAPS)," *Proceedings of the TOOLS-USA 2000*, 30 July-3 August 2000.
- Ge, J., Berzins, V., and Luqi, "Computer Aided Prototyping in a Distributed Environment," *Proceedings of the Symposium on Interactive and Collaborative Computing the International Congress on Intelligent Systems and Applications (ISA2000)*, Australia, 12-15 December 2000.

PRESENTATIONS:

- Shing, M., "Object-Oriented Modular Architecture for Ground Combat Simulation," 2000 Command and Control Research and Technology Symposium, Naval Postgraduate School, Monterey, CA, 26-28 June 2000.
- Harn, M., "A Formal Model for Software Evolution," 3rd International Conference on Computational Intelligence and Multimedia Applications, New Delhi, India, 23-26 September 1999.
- Harn, M., "Software Evolution Process via a Relational Hypergraph Model," IEEE/IEEJ/JSAI International Conference on Intelligent Transportation Systems, Tokyo, Japan, 5-8 October 1999.
- Nada, N., Berzins, V., and Luqi, "Automated Prototyping ToolKit," The 22nd International Conference on Software Engineering (ICSE2000), The 2nd International Symposium on Constructing Software Engineering Tools (COSET2000), Limerick, Ireland, 4-11 June 2000.
- Nada, N., Luqi, Rine, D., and Jaber, K., "Using Abstract Adapters for Distributed and Reusable Components," Distributed Networked Computing for a Secure Defense, Washington D.C., 24-25 April 2000.
- Nogueira, J., "Risk Assessment in Software Requirement Engineering," 5th World Conference on Integrated Design and Process Technology, Dallas, TX, 4-8 June 2000.
- Nogueira, J., "Surfing the Edge of Chaos: Applications to Software Engineering," 2000 Command and Control Research and Technology Symposium, Monterey, CA, 26-28 June 2000.
- Berzins, V., "A Formal Risk Assessment Model for Software Evolution," 2nd International Workshop on Economics-Driven Software Engineering Research (EDSER-2) of the 22nd International Conference on Software Engineering (ICSE2000), Limerick, Ireland, 4-10 June 2000.
- Luqi, "A Risk Assessment Model for Software Prototyping Projects," 11th IEEE International Workshop on Rapid System Prototyping (RSP2000), Paris, France, 21-13 June 2000.
- Nada, N., "Product Line Stakeholder Viewpoint and Validation Models," Workshop on Software Product Lines: Economics, Architectures, and Implications of the 22nd International Conference on Software Engineering (ICSE2000), Limerick, Ireland, 4-11 June 2000.

- Nada, N., "A Knowledge-Based System for Software Reuse Technology Practices," Third International Workshop on Intelligent Software Engineering (WISE3) of the 22nd International Conference on Software Engineering (ICSE2000), Limerick, Ireland, 4-11 June 2000.
- Nada, N., Berzins, V., and Luqi, "Automated Prototyping ToolKit," 22nd International Conference on Software Engineering (ICSE2000) and the 2nd International Symposium on Constructing Software Engineering Tools (COSET2000), Limerick, Ireland, 4-11 June 2000.
- Nada, N., "A Knowledge-Based Adaptive Distance Learning System for Software Reuse Technology," Twelfth International Conference on Software Engineering and Knowledge Engineering (SEKE2000), Chicago, 6-8 July 2000.
- Nada, N., "Using Abstract Adapters for Distributed and Reusable Components," Distributed Networked Computing for a Secure Defense, Washington D.C., 24-25 April 2000.
- Shing, M., "Computer Aided Prototyping System (CAPS) for Heterogeneous Systems Development and Integration," 2000 Command and Control Research and Technology Symposium, Naval Postgraduate School, Monterey, CA, 26-28 June 2000.
- Riehle, R., "Evolutionary Computer Aided Prototyping System (CAPS)," TOOLS-USA 2000, 30 July-3 August 2000.
- Ge, J., "Computer Aided Prototyping in a Distributed Environment," the Symposium on Interactive and Collaborative Computing, International Congress on Intelligent Systems and Applications (ISA2000), Australia, 12-15 December 2000.

THESES DIRECTED:

- Harn, M., "Computer-Aided Software Evolution Based on Inferred Dependencies," Ph.D. Dissertation, Naval Postgraduate School, December 1999.
- Lee, H., "Integrated Evolution Control System," Masters Thesis, Naval Postgraduate School, December 1999.
- Matsuo, E., "Risk Assessment in Incremental Software Development," Masters Thesis, Naval Postgraduate School, December 1999.
- Augustine, T., "Naval Architecture Environment: Facilitating JV2010," Masters Thesis, Naval Postgraduate School, December 1999.
- Kreeger, G., "Requirements Analysis and Design of a Distributed Architecture for the Computer-Aided Prototyping System (CAPS)," Masters Thesis, Computer Science, Naval Postgraduate School, September 1999
- Nogueira, J., "A Formal Model for Risk Assessment in Software Projects," Ph.D. Dissertation, Naval Postgraduate School, September 2000.
- Allen, J. and Tran, T., "Interoperability of COTS Software Components with Legacy Systems in a Distributed Computing Environment," Masters Thesis, Naval Postgraduate School, September 2000.
- Gee, K., "An Architectural Framework for Integrating COTS/GOTS/Legacy Systems," Masters Thesis, Naval Postgraduate School, June 2000.
- Nguyen, T., "Commercial Off-The-Shelf (Cots)/Legacy Systems Integration Architectural Design and Analysis," Masters Thesis, Naval Postgraduate School, September 2000.

DoD KEY TECHNOLOGY AREAS: Computing and Software

KEYWORDS: Software Requirements, Evolution, Prototyping, Embedded Systems

XML TECHNOLOGY ASSESSMENT Valdis Berzins, Professor Department of Computer Science Sponsor: Joint C4ISR Battle Center

OBJECTIVE: To evaluate and assess different methods for alleviating data interoperability problems in military systems.

SUMMARY: The JBC needs an assessment of technical issues related to the use of XML to achieve data interoperability in military systems. An XML schema should accommodate controlled change to enable incremental approaches to implementation that add one system at a time. If changes are done according to the least effort for each individual data interchange connection between legacy systems, the XML schema may become bloated with many different coding of the same information, which will eventually become a severe maintenance problem. The NPS Software Engineering Group proposes to evaluate and assess different methods for alleviating this problem.

We have investigated the use of XML for achieving data interoperability between DoD legacy systems from several points of view: methods for integrating XML schemas coving data interchange between pairs of systems, methods for using XML to transfer data between heterogeneous databases, and XML for data interchange between real-time systems. We have assessed the capabilities of commercial tools related to XML and XML interfaces to the commercial database systems used in the systems of interest to JBC. We have also assessed methods for translating between different XML representations of the same real-world data, corresponding to the different views of that data as modeled in different legacy systems.

PUBLICATION:

DaBose, M., "The Joint Technical Architecture Relationships and Implementation in Real Time Hard Time Systems," *Software Engineering Process Group Newsletter*, May 2000.

THESES DIRECTED:

Lyttle, B. and Ehrhardt, T., "Interconnectivity via a Consolidated Type Hierarchy and XML," Masters Thesis, Naval Postgraduate School, December 2000.

Hina, D., "Evaluation of the Extensible Markup Language (XML) as a Means for Establishing Interoperability between Homogeneous Department of Defense (DoD) Databases," Masters Thesis, Naval Postgraduate School, September 2000.

Gee, K., "An Architectural Framework for Integrating COT/GOTS/LEGACY Systems," Masters Thesis, Naval Postgraduate School, June 2000.

Tran, T.M. and Allen, J.O., "Interoperability and Security Support for Heterogeneous COTS/GOTS/Legacy Component-Based Architecture," Masters Thesis, Naval Postgraduate School, June 2000.

Nguyen, T.M., "Commercial-Off-The-Shelf (COTS)/Legacy Systems Integration Architectural Design and Analysis," Masters Thesis, Naval Postgraduate School, September 2000.

DoD KEY TECHNOLOGY AREAS: Computing and Software

KEYWORDS: Database, Interoperability, XML Schema

EVALUATION OF COTS ENTERTAINMENT SOFTWARE FOR ARMY RECRUITMENT

Michael Capps, Research Assistant Professor Department of Computer Science Sponsor: Office of Economic and Manpower Analysis

OBJECTIVE: COTS videogame software has great potential to aid Army recruiting and training efforts. However, there has to date been little collaboration between the Defense Department and the entertainment industry in this area. While there is significant interest in reproprosing COTS software for Army needs, this requires and investigation study into current technology and the ease with which this adaptation can be performed.

DoD KEY TECHNOLOGY AREAS: Computing and Software

KEYWORDS: Modeling and Simulation

SOFTWARE FRAMEWORK FOR COMPOSABLE AND SECURE VIRTUAL ENVIRONMENTS

Michael Capps, Research Assistant Professor Department of Computer Science Sponsor: Secretary of the Air Force

OBJECTIVE: We propose to develop systems architecture to support composable and extensible immersive virtual environments. This framework will allow development JOF Novel Application in the intelligence domain, both through composition of existing programs and rapid development of new applications. We additionally used this platform to explore new methods for security in virtual world telecollaboration.

DoD KEY TECHNOLOGY AREAS: Modeling and Simulation

KEYWORDS: Synthetic Environments, Virtual Environments, Modeling and Simulation

DIGITAL IMAGERY AND WIRELESS COMMUNICATIONS FOR LAND-BASED RECONNAISSANCE MISSIONS: A HUMAN FACTORS APPROACH

Rudy Darken, Assistant Professor

Department of Computer Science and Modeling and Virtual Environments,
and Simulation Academic Group

Sponsor: Center for Reconnaissance Research

OBJECTIVE: The use of streaming digital video and GPS data via wireless communications is proposed as a method of improving land-based reconnaissance. The ability to gather and disseminate reconnaissance data in its natural form and in a timely, comprehensible fashion is imperative to mission success. This proposal suggests a human factors-based approach whereby a task analysis is used to drive a prototype implementation. This prototype is to be evaluated with the cooperation of MCTSSA for utility and effectiveness. Lastly, methods of coordinating multiple streams of reconnaissance data into coherent tactical picture for the unit commander is needed to adequately capture crucial information form these non-standard form of data.

DoD KEY TECHNOLOGY AREAS: Computing and Software

KEYWORDS: Technology, Wearable Computing, Wireless Communications, Usability

MSHN: MANAGEMENT SYSTEM FOR HETEROGENEOUS NETWORKS

Cynthia E. Irvine, Assistant Professor
Department of Computer Science
Sponsor: Defense Advanced Research Projects Agency

OBJECTIVE: Research and design effort directed at solving the fundamental problems associated with and creating a distributed metacomputer.

SUMMARY: Phase I of the MSHN Project was completed in 2000. The accomplishments of the project include a peer-to-peer architecture composed of the following components: client library, scheduling advisor, resource requirements database, resource status server, MSHN daemon, and application emulator. The architecture supports the execution of many different client applications, both new and previously unencountered.

Mapping algorithm research supported the MSHN scheduler and resulted in the development of a "toolbox" of mapping techniques from which the scheduler can select the most appropriate algorithm for a given heterogeneous computing and application environment. A unified mapping framework was developed addressed two mapping problems: mapping with advance reservation and data replication, and mapping with resource co-allocation requirements.

MSHN produced a resource model that allows the system to make mapping decisions. Monitoring is needed to ensure that model represents the resources available. Strategies were developed to permit monitoring to be performed at each client. A number of techniques and tools were explored to permit the monitoring and modeling of communications resources.

The research explored the problem of distributed communications in an environment requiring transfers of large quantities of data. A uniform framework for developing communication schedules for collective communication patterns was introduced. The schedules were adapted at run-time, based on network performance information.

Performance metrics were developed so that the success of MSHN as a resource management system could be measured. A multi-dimensional performance measure was developed that included: priorities, task and data versions, deadlines, situational modes, security, and other dependencies.

Security was an integral part of the MSHN project. Multi-domain cryptographically enforced security architecture was developed that provided authentication and confidentiality for MSHN components. The notion of Quality of Security Service was introduced and developed as part of the project.

PUBLICATIONS:

Kim, J. -K., Hensgen, D., Kidd, T., Siegel, H.J., St. John, D., Irvine, C.E., Levin, T., Prasanna, V.K., and Freund, R. F., "A QoS Performance Measure Framework for Distributed Heterogeneous Networks," *Proceedings of EuroMocro-PDP*, Rhodos, Greece, January 2000, pp. 18-27.

Irvine, C.E., and Levin, T., "The Effects of Security Choices and Limits in a Metacomputing Environment," Naval Postgraduate School Technical Report, NPS-CS-00-004, April 2000.

Irvine, C.E., Siegel, H.J., Prasanna, V., Hensgen, D., and Levin, T., "Management System for Heterogeneous Networks Final Report, Volume I: Project Summary and Papers," NPS Technical Report NPS-CS-00-006, April 2000.

THESES DIRECTED:

Schaeffer, B., "Refining a Task-Execution Time Prediction Model for Use in MSHN," Masters Thesis, Naval Postgraduate School, March 2000.

Tsai, P., "Re-Targeting the Graze Performance Debugging Tool for Java Threads and Analyzing the Re-Targeting to Automatically Parallelized (FORTRAN) Code," Masters Thesis, Naval Postgraduate School, March 2000.

Polk, K., "Transparent Detection of QoS Violations for Continuous Applications," Masters Thesis, Naval Postgraduate School, June 2000.

DoD KEY TECHNOLOGY AREAS: Computing and Software

KEYWORDS: Heterogeneous, Distributed Computing, Data Staging, Metacomputing

MSHN: QUALITY OF SECURITY SERVICE FRAMEWORK

Cynthia E. Irvine, Assistant Professor
Department of Computer Science
Sponsor: Defense Advanced Research Projects Agency

OBJECTIVE: The objective of this research is to develop security architecture for management system for heterogeneous networks (MSHN) and, within the context of network quality of service, determine how requirements for security can be integrated into the task scheduling mechanism. The current research addresses: specification of security requirements, determination of possible job resources, costing of possible job resources, and selection of job resources to maximize benefit.

SUMMARY: A method for articulating network security functional requirements, and for measuring their fulfillment has been developed. Using this method, security in a quality of service framework (QoSS) is discussed in terms of variant security mechanisms and dynamic security policies. It was also shown how QoSS can be represented in a network scheduler benefit function.

A model for analyzing the relationship between the security services provided at the various network layers was developed and reflects the choices made by dependent layers as constrained by the limits imposed by underlying layers. In addition, a method for performing security allocation and assignment with respect to security choices made by metacomputer users and applications was presented.

Preliminary security service taxonomy was defined to provide the resource management system with potential resource utilization costs. Based upon this taxonomy, we developed a framework for defining the costs of various network services.

The problem of how users and administrators can easily interact with the wide range of security resources and mechanisms was addressed. A method for translation of a simplified user abstraction of security to detailed underlying mechanisms was formulated.

An approach for representing the level of resources consumed by jobs under the control of a resource management system was developed. This work showed how this measurement of resource usage can be combined with a notion of user preferences to reflect a restrictive resource-usage policy for network management.

PUBLICATIONS:

Spyropoulou, E., Levin, T., and Irvine, C.E., "Calculating Costs for Quality of Security Service," *Proceedings of the 16th Computer Security Applications Conference*, New Orleans, LA, December 2000, pp. 334-343.

Irvine, C.E. and Levin, T., "Quality of Security Service," *Proceedings of the New Security Paradigms Workshop*, September 2000, pp. 91-99.

Irvine, C.E. and Levin, T., "An Argument for Quality of Security Service," *Proceedings of the National Computer Security Conference*, Baltimore, MD, October 2000, p. 519.

Irvine, C.E. and Levin, T., "Toward Quality of Security Service in a Resource Management System Benefit Function," *Proceedings of the 2000 Heterogeneous Computing Workshop*, Cancun, Mexico, May 2000, pp. 18-27.

Irvine, C.E. and Levin, T., *Introduction to Quality of Security Service*, Naval Postgraduate School Technical Report, NPS-CS-00-005, April 2000.

Spyropoulou, E., Levin, T., and Irvine, C.E., *Quality of Security Service Costing Demonstration for the MSHN Project*, Naval Postgraduate School Technical Report, NPS-CS-00-007, April 2000.

DoD KEY TECHNOLOGY AREAS: Computing and Software

KEYWORDS: Heterogeneous, Distributed Computing, Data Staging, Metacomputing

SUPPORT FOR NPS CISR INFORMATION ASSURANCE RESEARCH PROGRAM

Cynthia E. Irvine, Assistant Professor
Department of Computer Science
Sponsor: Defense Information Systems Agency

OBJECTIVE: This project is to support research in information assurance at the Naval Postgraduate School Center for INFOSEC Studies and Research. The research will include work on high assurance multi-level servers, high assurance network authentication, authentication challenges relating to firewalls and an advanced topics short course.

SUMMARY: Results from this research-included examination of user-friendly interfaces for use in systems enforcing label-based policies. Criteria were established to assess the usability of e-mail clients in a label-based context. Popular commercial-off-the-shelf mail clients were evaluated under these criteria and significant differences in usability were found.

In the area of authentication, a framework for high-speed packet authentication was developed that uses a low-overhead temporal method of updating keys that reduces requirements for time-durability of keys. The method accounts for clock drift and network latency. Sufficiency of the derived conditions to protect data and to ensure data deliverability was demonstrated.

A set of topics and preliminary notes for the short course were developed. The course will be presented in the spring of FY01.

PUBLICATIONS:

Irvine, C.E., "Security: Where Testing Fails," ITEA Journal, June 2000, pp. 53-57.

Irvine, C.E., "An Argument for Academic Research in Information Security," *Proceedings of the National Information Systems Security Conference*, Baltimore, MD, October 2000, pp. 710-711.

THESIS DIRECTED:

Everett, T., "Enhancement of Internet Message Access Protocol (IMAP) for User-Friendly Multi-level Mail Management," Masters Thesis, Naval Postgraduate School, September 2000.

DoD KEY TECHNOLOGY AREAS: Computing and Software, Other (Information Assurance)

KEYWORDS: Computer Security, Information System Security, INFOSEC, Information Assurance, Network Security

NAVY IWD/INFOSEC/IA SUPPORT PLAN FOR NPS CISR

Cynthia E. Irvine, Assistant Professor

Department of Computer Science

Sponsors: Chief of Naval Operations (N63) and Naval Postgraduate School

OBJECTIVE: The objective of this research is to provide support for the Naval Postgraduate School Center for INFOSEC Studies and Research (NPS CISR) in an integrated approach to INFOSEC research and education that focuses on important computer and network security problems of DoN and DoD. Thus serving the needs of the warfighter. Information warfare defense and Information Assurance (IA) objectives of the DoN are supported through a cadre of officers who have conducted coursework and research in INFOSEC and IA as well as through the ongoing research results produced by NPS CISR.

SUMMARY: Student research supported by this work included an exploration of a Java-based implementation of the new Advanced Encryption Standard, Rinjdael on the iButton, of Dallas Semiconductor. Performance analysis demonstrated that the cost of using the iButton was high for an unoptimized implementation. Among the implementation challenges were the absence of general support for matrix operations, upon which the AES algorithm is dependent.

Several ongoing projects intended to support the emerging DoD public key infrastructure (PKI) were started. These included an examination of the feasibility of the use of the PKI in tactical situations. Another study involves configuration management issues for deployed PKI components. A third research effort is exploring metrics for the service level agreement (SLA) for operational services relating to the PKI that are required for the Navy Marine Corps Internet.

Human factors in the perceived and actual level of security awareness are the topic of another investigation. A survey is being developed which will assess security awareness and then a plan to improve security awareness will be recommended.

Highly trustworthy user interfaces for an open source operating system constituted another area within the scope of this research. The objective was to identify all of the mechanisms within the keyboard interface that represent trap doors in the open source system and to modify the design of the input subsystem so that a trustworthy secure attention key was possible. Additionally, this work resulted in the development of a state representation of the interface that could be used for subsequent design of a trusted path interface.

PUBLICATIONS:

Irvine, C. E., "Security Issues for Automated Information Systems," *Handbook of Public Information Systems*, D. Garson, ed., Marcel Dekker, Inc., New York, NY, pp. 231-245, 2000.

Clark, P., "Supporting Mandatory Access Control in an Educational Environment," *Proceedings of the National Information Systems Security Conference*, October 2000.

THESIS DIRECTED:

Bartram, S., "Supporting a Trusted Path for the Linux Operating System," Masters Thesis, Naval Postgraduate School, June 2000.

DoD KEY TECHNOLOGY AREAS: Computing and Software, Other (Information Assurance)

KEYWORDS: Computer Security, Information System Security, INFOSEC, Information Assurance, Network Security

HIGH ASSURANCE LABEL PROCESSING MAIL SERVICE

Cynthia E. Irvine, Assistant Professor Department of Computer Science Sponsor: Naval Engineering Logistics Office

OBJECTIVE: This research is to develop a prototype demonstration of a basic label processing mail service on a high assurance trusted base. The demonstration will show how a mail service can separate internal/external and secret/unclassified information with high assurance. It is intended to be an initial component of high assurance network security architecture for office automation that will allow the use of COTS applications and operating systems.

SUMMARY: This work resulted in the development of a requirements specification and high-level design specification for a communications protocol. The requirements specification process used a threat model that included both operational and developmental threats. In addition the specification approach addressed both functional and non-functional security requirements. The requirements specification process was iterative and used the design specification as the next stage of system refinement. Notions that were insufficiently abstract were moved to the design specification, while requirements that could be generalized were moved to the requirements specification. Members of the design group played the role of stakeholders in the design process. To ensure that the system specifications were realistic, gedanken experiments were used as part of the process.

Two trusted server processes were completed and tuned for performance. One was the TCB Extension server, which is intended to provide server-side support for a high assurance protected communications channel between the user and the TCB. This server managed the session database that contained client session attributes such as user identification and session level. The other was a secure session server. This trusted module referenced the session database to assign attributes to application protocol servers that were instantiated on behalf of client systems.

Analysis of the security requirements for a TCB Extension was conducted. A prototype board was selected. It is a plug-in board compatible with the 440BX motherboard of the PC architecture. The plug-in board, which supports an Intel i960 processor, can act either as a PCI bridge or as a secure gateway between the PC and the network. The reference monitor properties of the board were examined and it was concluded that the board can be configured to be both non-by passable and tamper resistant by malicious software. A series of experiments were performed to demonstrate these conclusions. In one, the PCI bridge is shut down by setting the base address and the limit for its buffers to the same value. In the other a NMI, which would provide a Secure Attention Key (SAK) was simulated and forced the shutdown of the bridge. Thus it was demonstrated that a SAK could be associated with the plug-in board.

Low-level object reuse on the client PC was examined and several memory areas that would require purging between sessions with differing security attributes were identified. Techniques to initiate purges from an add-on TCB extension were explored. Overwriting, flushing, and memory latency manipulation were among the techniques identified to remove potentially sensitive information from memory.

PUBLICATION:

Balmer, S.R. and Irvine, C.E., "Analysis of Terminal Server Architectures for Thin Clients in a High Assurance Network," *Proceedings National Information Systems Security Conference*, October 2000, pp. 192-202.

THESES DIRECTED:

Brown, E. "Implementation of an SMPT Server for a High Assurance Multi-level LAN," Masters Thesis, Naval Postgraduate School, September 2000.

Rossetti, R., "A Mail File Administration Tool for a Multi-level High Assurance LAN," Masters Thesis, Naval Postgraduate School, September 2000.

Wilson, J.D., "Trusted Networking in a Multi-level Secure Environment," Masters Thesis, Naval Postgraduate School, June 2000.

Agacayack, C., "Controlling Object Reuse in Clients Supported by a Trusted Computer Base Extension," Masters Thesis, Naval Postgraduate School, March 2000.

Turan, B., "Client Bootstrap Under Trusted Computing Base Extension Control," Masters Thesis, Naval Postgraduate School, March 2000.

DoD KEY TECHNOLOGY AREAS: Computing and Software, Other (Information Assurance)

KEYWORDS: Multi-level Security, Network Security, Distributed Systems Security, COTS Security

HIGH ASSURANCE DISTRIBUTED MULTI-LEVEL COMPUTING ENVIRONMENT, PHASE II

Cynthia E. Irvine, Assistant Professor
Department of Computer Science
Sponsor: Naval Engineering Logistics Office

OBJECTIVE: This project is to continue work in support of a high assurance distributed multi-level computing environment, building on recent work accomplished on the Naval Postgraduate School High Assurance Label Processing Mail Service Prototype undertaken during Phase I. Areas of study include applicability to collaborative environments, extension of label processing, trusted path extensions, and supporting policy adaptations.

SUMMARY: A study was made of the impact of using commercial-off-the-shelf (COTS) software in the context of a high assurance environment that supports controlled sharing of information by entities in well defined dominance domains. A set of architectures was identified and for these architectures we showed that, while they are capable of supporting multi-level confidentiality policies, they do not generally support partially ordered integrity policies. The applicability of high assurance architectures for the support of integrity is limited by the integrity of the COTS components.

An Apache-based, security-aware web server was developed for a high assurance platform. It was demonstrated that this web server could provide information at or below the session level of properly authenticated network clients.

As part of the network architectural study, a security requirements document was developed. This document reflected a strategy for security requirements engineering based upon a threat model that incorporated developmental and operational threats. We asserted that because some security requirements cause a change in system state, they can be characterized as functional. The requirements that emerged from the process addressed both functional and non-functional concerns.

PUBLICATIONS:

Irvine, C.E. and Levin, T., "Data Integrity Limitations in Hybrid Security Architectures," Naval Postgraduate School Technical Report, NPS-CS-00-008, December 2000.

Irvine, C.E. and Levin, T., "Data Integrity Limitations in Hybrid Security Architectures," to appear in *Proceedings of the International System Security Engineering Conference*, Orlando, FL, February-March 2000.

Irvine, C.E., Levin, T., Wilson, J.D., Shifflett, D., and Pereira, B., "A Case Study in Security Requirements Engineering for a High Assurance System," to appear in *Proceedings of the System Requirements Engineering in Information Assurance Symposium*, Indianapolis, IN, March 2000.

THESIS DIRECTED:

Bersack, E., "Implementation of a HTTP (Web) Server on a High Assurance Multi-level Secure Platform," Masters Thesis, Naval Postgraduate School, December 2000.

DoD KEY TECHNOLOGY AREAS: Computing and Software, Other (Information Assurance)

KEYWORDS: Multi-level Security, Network Security, Distributed Systems Security, COTS Systems

NPS CENTER FOR INFOSEC STUDIES AND RESEARCH

Cynthia E. Irvine, Assistant Professor Department of Computer Science Sponsors: National Security Agency

OBJECTIVE: The objective of this research is to provide sustained support for the Naval Postgraduate School Center for Information Systems Security (INFOSEC) Studies and Research in the areas of curriculum development, trusted systems laboratory development, faculty development in INFOSEC and Information Assurance, a visiting professor program, an invited lecture series, academic outreach, and graduate utilization. It provides an integrated approach to INFOSEC research and education that focuses important problems of DoN, DoD, and U.S. government, thus serving the needs for the warfighter and intelligence community.

SUMMARY: Research to develop security enhancements for the Linux operating system continued. A framework to add labels to file system objects and to subjects (active system entities) was completed. Work continued on the creation of a trusted path mechanism for Linux. The specification of the trusted path was completed.

Research collaboration between C. Irvine and G. Xie (NPS Computer Science Department) continued with the method for rapid authentication of IP datagrams in high-speed networks. The technique uses rapid changes to key tables for the authentication algorithm.

The broad NPS CISR effort in the area of computer security education continued and included development or improvement of intermediate and advanced graduate courses in computer security, an invited lecture series on computer security topics, and participation in regional and national computer security education activities.

NPS CISR hosted 12 invited lectures during 2000. All were recorded and archived onto CD ROM, which have been made available to sponsors.

Course materials were extended and updated to reflect changes in technology and advances in the areas of network and computer security.

PUBLICATIONS:

Irvine, C.E. and Levin, T., "Is Electronic Privacy Achievable?" *Proceedings of the IEEE Symposium on Security and Privacy*, Oakland, CA, May 2000, pp. 76-77.

Robin, J.S. and Irvine, C.E., "Analysis of the Intel Pentium's Ability to Support a Secure Virtual Machine Monitor," *Proceedings of the 9th Usenix Security Symposium*, Denver, CO, August 2000, pp. 129-144.

DoD KEY TECHNOLOGY AREAS: Computing and Software, Other (Information Assurance)

KEYWORDS: Computer Security, Information System Security, INFOSEC, Information Assurance, Network Security

SYSTEM ENGINEERING AND EVOLUTION DECISION SUPPORT

Luqi, Professor Department of Computer Science

Sponsor: U. S. Army Research Office and Naval Postgraduate School

OBJECTIVE: The objectives of this research is to develop a scientific basis for system engineering automation and decision support, with the long term goals of increasing the quality of service provided complex systems while reducing development risks, costs, and time.

SUMMARY: The goal of our research is to develop an integrated set of formal models and methods for system engineering automation. These results will enable building decision support tools for concurrent engineering. Our research addresses complex modular systems with embedded control software and real-time requirements.

We focused on automation of design activities that appear in an evolutionary approach to system development. Decision support for design synthesis, reuse and evolution is emphasized. This research extended recently developed formal methods in system engineering to construct a cohesive set of formal models. These models are used to create and to connect automated processes for computer aided prototyping, requirements validation, and design synthesis. Mathematical models for implementing a set of automated and integrated engineering automation tools were also developed. Our work combined veryhigh-level specification abstractions and concepts with: (1) formal real-time models, (2) automated management of system design data and human resources, (3) design transformations, (4) change merging, (5) automated retrieval of reusable system design components, and (6) automated schedule construction. We have created automated methods for: (1) generating real-time control programs, (2) generating simulations of subsystems, and (3) coordinating concurrent work by engineering teams. Our work will ensure design consistency and to alleviate communication difficulties. The significance of our work is to: 1) improve system effectiveness and flexibility, 2) increase engineering productivity, 3) reduce system maintenance costs.

This was achieved by providing a higher level of engineering automation coupled directly with requirements validation facilities. Our work will broaden the scope of engineering decision support to include concurrent whole-system engineering, requirement determination, and system evolution. Automated decision support will ensure system quality by decreasing the human effort required. This, in turn, will minimize the incidence of human error. The trial use of operational system prototypes linked with software simulations of selected subsystems enables users to provide feedback for validation and refinement of system requirements prior to detailed design. Maintenance costs can be minimized by reducing the need to repair requirement errors after system deployment. We provided methods for process and system re-engineering at minimal cost. This was achieved by: (1) regenerating new variations of designs from high-level decisions. (2) combining changes, and (3) propagating the consequences of design modifications. These engineering capabilities will enable the Army to improve and integrate its complex systems with reduced costs. Improved systems can reduce Army manpower needs while strengthening information warfare capabilities.

Specific tasks accomplished in FY00 include (1) the development of a risk assessment model for the evolutionary software process; (2) a detailed survey of the software reuse repositories, (3) the development of models to support reuse in product line approach, and (4) tool enhancements for system engineering and evolution decision support.

PUBLICATIONS:

Berzins, V., Shing, M., Luqi, Saluto, M., and Williams, J., "Architectural Re-Engineering of Janus Using Object Modeling and Rapid Prototyping," *Design Automation for Embedded Systems*, 5(3/4), August 2000, pp. 251-263.

Berzins, V., Shing, M., Luqi, Saluto, M., and Williams, J., "Object-Oriented Modular Architecture for Ground Combat Simulation," *Proceedings of the 2000 Command and Control Research and Technology Symposium*, Naval Postgraduate School, Monterey, CA, 26-28 June 2000.

Berzins, V., "Static Analysis for Program Generation Templates," *Proceedings of 7th Monterey Workshop: Modeling Software System Structures in a Fast Moving Scenario*, Santa Margherita Ligure, Italy, 13-16 June 2000.

Guo, J. and Luqi, "Reuse and Re-Engineering of Legacy Systems," *Proceedings of the 5th World Conference on Integrated Design and Process Technology*, Dallas, TX, 4-8 June 2000.

Guo, J. and Luqi, "A Survey of Software Reuse Repositories," *Proceedings of the 7th IEEE International Conference and Workshop on the Engineering of Computer Based Systems (IEEE ECBS 2000)*, Edinburgh, Scotland, UK, 6-7 April 2000.

Luqi and Nogueira, J.C., "A Risk Assessment Model for Evolutionary Software Projects," *Proceedings of 7th Monterey Workshop: Modeling Software System Structures in a Fast Moving Scenario*, Santa Margherita Ligure, Italy, 13-16 June 2000.

Luqi, Berzins, V., Shing, M., Riehle, R., and Nogueira, J.C., "Evolutionary Computer Aided Prototyping System (CAPS)," *Proceedings of the TOOLS USA 2000 Conference*, Santa Barbara, CA, 30 July-3 August 2000.

Luqi, Berzins, V., Shing, M., Saluto, M., Williams, J., Guo, J., and Shultes, B., "The Use of Computer Aided Prototyping for Re-Engineering Legacy Software," submitted to *IEEE Transactions on Software Engineering*.

Nada, N., Luqi, Rine, D., and Jaber, K., "Product Line Stakeholder Viewpoint and Validation Models," *Proceedings of the* Workshop *on Software Product Lines: Economics, Architectures, and Implications*, Limerick, Ireland, 4-11 June 2000.

Nada, N., Luqi, Rine, D., and Damiani, E., "A Knowledge-Based System for Software Reuse Technology Practices," *Proceedings of the Third International Workshop on Intelligent Software Engineering (WISE3)*, Limerick, Ireland, 4-11 June 2000.

Nogueira, J.C., Luqi, and Berzins, V., "Risk Assessment in Software Requirement Engineering," *Proceedings of the 5th World Conference on Integrated Design & Process Technology*, Dallas, TX, 4-8 June 2000.

Nogueira, J.C., Jones, C., and Luqi, "Surfing the Edge of Chaos: Applications to Software Engineering," *Proceedings of the 2000 Command and Control Research and Technology Symposium*, Monterey, CA, 26-28 June 2000.

Nogueira, J.C., Luqi, Berzins, V., and Nada, N., "A Formal Risk Assessment Model for Software Evolution," *Proceedings of the 2nd International Workshop on Economics-Driven Software Engineering Research (EDSER-2)*, Limerick, Ireland, 4-11 June 2000.

Nogueira, J.C., Luqi, and Bhattacharya, S., "A Risk Assessment Model for Software Prototyping Projects," *Proceedings of the 11th IEEE International Workshop on Rapid System Prototyping*, Paris, France, 21-23 June 2000.

Luqi, "System Engineering and Evolution Decision Support - Interim Progress Report (01/01/2000 – 09/30/2000)," Naval Postgraduate School Technical Report, NPS-SW-00-001, Naval Postgraduate School, September 2000.

PRESENTATIONS:

Shing, M., "Object-Oriented Modular Architecture for Ground Combat Simulation," 2000 Command and Control Research and Technology Symposium, Naval Postgraduate School, Monterey, CA, 26-28 June 2000.

Berzins, V., "Static Analysis for Program Generation Templates," 7th Monterey Workshop: Modeling Software System Structures in a Fast Moving Scenario, Santa Margherita Ligure, Italy, 13-16 June 2000.

Guo, J., "Reuse and Re-engineering of Legacy Systems," 5th World Conference on Integrated Design & Process Technology, Dallas, TX, 4-8 June 2000.

Guo, J., "A Survey of Software Reuse Repositories," 7th IEEE International Conference and Workshop on the Engineering of Computer Based Systems (IEEE ECBS 2000), Edinburgh, Scotland, UK, 6-7 April 2000.

Luqi, "A Risk Assessment Model for Evolutionary Software Projects," 7th Monterey Workshop: Modeling Software System Structures in a Fast Moving Scenario," Santa Margherita Ligure, Italy, 13-16 June 2000.

Riehle, R., "Evolutionary Computer Aided Prototyping System (CAPS)," TOOLS USA 2000 Conference, Santa Barbara, CA, 30 July–3 August 2000.

Nada, N., "Product Line Stakeholder Viewpoint and Validation Models," Workshop on Software Product Lines: Economics, Architectures, and Implications, Limerick, Ireland, 4-11 June 2000.

Nada, N., "A Knowledge-Based System for Software Reuse Technology Practices," Third International Workshop on Intelligent Software Engineering (WISE3), Limerick, Ireland, 4-11 June 2000.

Nogueira, J.C., "Risk Assessment in Software Requirement Engineering," 5th World Conference on Integrated Design and Process Technology, Dallas, TX, 4-8 June 2000.

Nogueira, J.C., "Surfing the Edge of Chaos: Applications to Software Engineering," 2000 Command and Control Research and Technology Symposium, Monterey, CA, 26-28 June 2000.

Berzins, V., "A formal Risk Assessment Model for Software Evolution," 2nd International Workshop on Economics-Driven Software Engineering Research (EDSER-2), Limerick, Ireland, 4-11 June 2000.

Luqi, "A Risk Assessment Model for Software Prototyping Projects," 11th IEEE International Workshop on Rapid System Prototyping, Paris, France, 21-23 June 2000.

THESIS DIRECTED:

Nogueira, J.C., "A Formal Model for Risk Assessment in Software Projects," Ph.D. Dissertation, Naval Postgraduate School, September 2000.

DoD KEY TECHNOLOGY AREAS: Computing and Software

KEYWORDS: System Engineering, Software Evolution, Decision Support, Concurrent Engineering

COMPUTER-AIDED ENGINEERING OF HETEROGENEOUS SYSTEMS

Luqi, Professor

Department of Computer Science

Sponsor: Defense Advanced Research Projects Agency and Naval Postgraduate School

OBJECTIVE: To develop improved methods for engineering and constructing heterogeneous systems and environments.

SUMMARY: This project seeks improved methods to: speed up design and construction, support integration and evolutionary expansion, evaluated and improve performance, and demonstrate

improvements via a case study. We tackled the problem using prototyping and a "wrapper and glue" technology for the engineering and integration of heterogeneous systems. Our approach is based on a distributed architecture where components collaborate via message passing over heterogeneous networks. It uses a generic interface that allows system designers to specify communication and operating requirements between components as parameters, based on properties of COTS/GOTS components. A separate parameterized model of network characteristics constrains the concrete "glue" software generated for each node. The model enables partial specification of requirements by the system designers, and allows them to explore design alternatives and determine missing parameters via rapid prototyping.

The cornerstone of our approach is automatic generation of wrapper and glue software based on designer specifications. This software bridges interoperability gaps between individual COTS/GOTS components. Wrapper software provides a common message-passing interface for components that frees developers from the error prone tasks of implementing interface and data conversion for individual components. The glue software schedules time-constrained actions and carries out the actual communication between components.

Specific tasks accomplished in FY00 include (1) the design of an interface wrapper model that allows developers to treat distributed objects as local objects, (2) the development of a tool to generate Java interface wrapper from a specification written in the high-level Prototype System Description Language (PSDL), (3) the design of a distributed heterogeneous environment to automate the process of integration distributed systems, (4) a case study involving the development of a "wrapper and glue" solution for integrating/extending COTS/GOTS/legacy components of the Naval Integrated Tactical Environmental System I (NITES I), and (5) the design of high-level net models for fault detection in multistage interconnected networks.

PUBLICATIONS:

Ge, J., Berzins, V., and Luqi, "Computer Aided Prototyping in a Distributed Environment," *Proceedings of the International Congress on Intelligent Systems and Applications (ISA2000)*, to appear in *Proceedings of the Symposium on Interactive and Collaborative Computing*, Australia, 12-15 December 2000.

Cheng, N., Berzins, V., Luqi, and Bhattacharya, S., "Automated Generation of Wrappers for Interoperability," *Proceedings of the 2000 Command and Control Research and Technology Symposium*, Monterey, CA, 26-28 June 2000.

Luqi, Berzins, V., Shing, M., Nada, N., and Eagle, C., "Computer Aided Prototyping System (CAPS) for Heterogeneous Systems Development and Integration," *Proceedings of the 2000 Command and Control Research and Technology Symposium*, Monterey, CA, 26-28 June 2000.

Nada, N., Berzins, V., and Luqi, "Prototyping Tool-Kit (APT)," *Proceedings of the 2nd International Symposium on Constructing Software Engineering Tools (CoSET 2000)*, ICSE 2000, Limerick, Ireland, 4-11 June 2000.

Ge, J., "Computer Aided Prototyping in a Distributed Environment," International Congress on Intelligent Systems and Applications (ISA2000); to appear in *Proceedings of the Symposium on Interactive and Collaborative Computing*, Australia, 12-15 December 2000.

PRESENTATIONS:

Bhattacharya, S., "Automated Generation of Wrappers for Interoperability," 2000 Command and Control Research and Technology Symposium, Monterey, CA, 26-28 June 2000.

Shing, M., "Computer Aided Prototyping System (CAPS) for Heterogeneous Systems Development and Integration," 2000 Command and Control Research and Technology Symposium, Monterey, CA, 26-28 June 2000.

Berzins, V., "Prototyping Tool-Kit (APT)," 2nd International Symposium on Constructing Software Engineering Tools (CoSET 2000), ICSE 2000, Limerick, Ireland, 4-11 June 2000.

THESES DIRECTED:

Allen, J. and Tran, T., "Interoperability of COTS Software Components with Legacy Systems in a Distributed Computing Environment," Masters Thesis, Naval Postgraduate School, September 2000.

Franco, R., "Second Generation Ultra High Frequency (UHF) Satellite Protocol," Masters Thesis, Naval Postgraduate School, June 2000.

Gee, K., "An Architectural Framework for Integrating COTS/GOTS/Legacy Systems," Masters Thesis, Naval Postgraduate School, June 2000.

Nguyen, T., "Commercial-Off-The-Shelf (COTS)/Legacy Systems Integration Architectural Design and Analysis," Masters Thesis, Naval Postgraduate School, September 2000.

Cheng, N., "Automated Generation of Wrappers for Interoperability," Masters Thesis, Naval Postgraduate School, June 2000.

DoD KEY TECHNOLOGY AREAS: Computing and Software

KEYWORDS: System Engineering, Software, Decision Support, Heterogeneous Systems

ENGINEERING AUTOMATION FOR RELIABLE SOFTWARE

Luqi, Professor Department of Computer Science Sponsor: U.S. Army Research Office

OBJECTIVE: To develop technology for reliable software development through the automatic generation of glue and wrappers based on designer's specifications.

SUMMARY: This project addresses the problem of how to produce reliable software that is also flexible and cost effective for the DoD distributed software domain. Current and future DoD software systems fall into two categories: information systems and warfighter systems. Both kinds of systems can be distributed, heterogeneous and network-based, consisting of a set of components running on different platforms and working together via multiple communication links and protocols.

We focused on "wrap and glue" technology based on a domain specific distributed prototype model. Glue and wrappers consists of software that bridges the interoperability gap between individual COTS/GOTS components. The key to making the proposed approach reliable, flexible, and cost-effective is the automatic generation of glue and wrappers based on a designer's specification. The proposed "wrap and glue" approach allows system designers to concentrate on the difficult interoperability problems and defines solutions in terms of deeper and more difficult interoperability issues, while freeing designers from implementation details. The objective of our research is to develop an integrated set of formal models and methods for systems engineering automation. These results will enable building decision support tools for concurrent engineering. Our research addresses complex modular systems with embedded control software and real-time requirements.

Our long-term goals are to construct an integrated set of software tools that can improve software quality and flexibility by automating a significant part of the process and providing substantial decision support for the aspects that cannot be automated. The resulting development environment should be adaptable to enable (1) maintaining integrated support in the presence of business process improvement, (2) incorporation of future improvements in engineering automation methods, and (3) specialization to particular problem domains.

Specific tasks accomplished in FY00 include (1) the design of an interface wrapper model that allows developers to treat distributed objects as local objects, (2) the development of a tool to generate Java interface wrappers from a specification written in the high-level Prototype System Description Language (PSDL), (3) the design of a distributed heterogeneous environment to automate the process of integration

distributed systems, (4) a case study involving the development of a "wrapper and glue" solution for integrating/extending COTS/GOTS/legacy components of the Naval Integrated Tactical Environmental System I (NITES I), (5) the design of high-level net models for fault detection in multi-stage interconnected networks, (6) tools for assertion checking, dynamic analysis and testing of programs, (7) application of machine learning algorithms in software development, and (8) reliability modeling for safety critical software.

PUBLICATIONS:

Auguston, M., "Assertion Checker for the C Programming Language Based on Computations Over Event Traces," *Proceedings of the Fourth International Workshop on Algorithmic and Automatic Debugging*, AADEBUG'2000, Munich, Germany, 28-30 August 2000.

Auguston, M., "Tools for Program Dynamic Analysis, Testing, and Debugging Based on Event Grammar," *Proceedings of the 12th International Conference on Software Engineering and Knowledge Engineering*, Chicago, IL, 6-8 July 2000, pp.159-166.

Auguston, M., "Lightweight Semantics Models for Program Testing and Debugging Automation," *Proceedings of 7th Monterey Workshop: Modeling Software System Structures in a Fast Moving Scenario*, Santa Margherita Ligure, Italy, 13-16 June 2000.

Auguston, M., "Building Program Behavior Models," submitted to the *Journal Applied Intelligence* for the Special Issue on Spatial and Temporal Reasoning, 2000.

Berzins, V., "Static Analysis for Program Generation Templates," *Proceedings of 7th Monterey Workshop: Modeling Software System Structures in a Fast Moving Scenario*, Santa Margherita Ligure, Italy, 13-16 June 2000.

Chaki, N. and Bhattacharya, S., "High Level Net Models: A Tool for Fault-Detection in Multi-stage Interconnection Network," *Proceedings of the IEEE Region 10 Conference (TENCON) 2000*, Kuala Lumpur, Malaysia, 24-27 September 2000.

Cheng, N., Berzins, V., Luqi, and Bhattacharya, S., "Automated Generation of Wrappers for Interoperability," *Proceedings of the 2000 Command and Control Research and Technology Symposium*, Monterey, CA, 26-28 June 2000.

Ge, J., Berzins, V., and Luqi, "Computer Aided Prototyping in a Distributed Environment," *Proceedings of the International Congress on Intelligent Systems and Applications (ISA2000)*, to appear in *Proceedings of the Symposium on Interactive and Collaborative Computing*, Australia, 12-15 December 2000.

Gregory, J., Zhang, D., and Lu, M., "A Framework for Natural Language Agents," *Proceedings of Ninth International Conference on Intelligent Systems*, Louisville, KY, June 2000, pp. 57-60.

Kiselyov, O., "Implementing Metcast in Scheme," *Proceedings of the Workshop on Scheme and Functional Programming*, Montréal, Canada, September 2000, pp. 23-25.

Kitchenham, B. and Schneidewind, N., "Towards an Ontology of Software Maintenance," *Journal of Software Maintenance: Research and Practice*, Vol. 11, 1999, pp. 365-389.

Luqi, Berzins, V., Shing, M., Nada, N., and Eagle, C., "Computer Aided Prototyping System (CAPS) for Heterogeneous Systems Development and Integration," *Proceedings of the 2000 Command and Control Research and Technology Symposium*, Monterey, CA, 26-28 June 2000.

Luqi and Nogueira, J. C., "A Risk Assessment Model for Evolutionary Software Projects," *Proceedings of 7th Monterey Workshop: Modeling Software System Structures in a Fast Moving Scenario*, Santa Margherita Ligure, Italy, 13-16 June 2000.

Nada, N., Berzins, V., and Luqi, "Prototyping Tool-Kit (APT)," *Proceedings of the 2nd International Symposium on Constructing Software Engineering Tools (CoSET 2000), ICSE 2000*, Limerick, Ireland, 4-11 June 2000.

Pramanik, S., Choudhury, S., Chaki, N., and Bhattacharya, S., "Conceptual Level Graph Theoretic Design and Development of Complex Information System," *Proceedings of the IEEE International Conference on Information Technology: Coding and Computing (ITCC'00)*, Las Vegas, NV, 27-29 March 2000.

Schneidewind, N., "Measuring and Evaluating Maintenance Process Using Reliability, Risk, and Test Metric," *IEEE Transactions on Software Engineering*, Vol. 25, No. 6, November/December 1999, pp. 769-781.

Schneidewind, N., "Cost Framework for COTS Evaluation," *Proceedings of COMPSAC 99*, Phoenix, AZ, 27 October 1999, pp. 100-101.

Schneidewind, N. and Nikora, A., "Predicting Deviations in Software Quality By Using Relative Critical Value Deviation Metrics," *Proceedings of the 10th International Symposium on Software Reliability Engineering*, Boca Raton, FL, 1-4 November 1999, pp. 136-146.

Schneidewind, N., "Investigation of the Risk to Software Reliability of Requirements Changes," *Proceedings of the 1999 NASA Workshop on Risk Management*, Morgantown, WV, 28-29 October 1999.

Schneidewind, N., "Reliability Modeling for Safety Critical Software," *Proceedings of the 12th Annual Software Technology Conference*, Salt Lake City, UT, 30 April-5 May 2000.

Schneidewind, N., "Software Quality Control and Prediction Model for Maintenance," *Annals of Software Engineering*, Vol. 9, 2000, pp. 79-101.

Schneidewind, N., "The Ruthless Pursuit of the Truth about COTS," *Proceedings of the North Atlantic Treaty Organization, Commercial Off-The-Shelf Products in Defense Applications*, Brussels, Belgium, 3-5 April 2000.

Zhang, D. and Luqi, "Approximate Declarative Semantics for Rule Base Anomalies," *Knowledge-Based Systems*, Vol.12, No.7, November 1999, pp. 341-353.

Zhang, D., "Applying Machine Learning Algorithms in Software Development," *Proceedings of 7th Monterey Workshop: Modeling Software System Structures in a Fast Moving Scenario*, Santa Margherita Ligure, Italy, 13-16 June 2000.

PRESENTATIONS:

Auguston, M., "Assertion Checker for the C Programming Language based on Computations Over Event Traces," Fourth International Workshop on Algorithmic and Automatic Debugging, AADEBUG 2000, Munich, Germany, 28-30 August 2000.

Auguston, M., "Tools for Program Dynamic Analysis, Testing, and Debugging Based on Event Grammars," 12th International Conference on Software Engineering and Knowledge Engineering, Chicago, IL, 6-8 July 2000.

Auguston, M., "Lightweight Semantics Models for Program Testing and Debugging Automation," 7th Monterey Workshop: Modeling Software System Structures in a Fast Moving Scenario, Santa Margherita Ligure, Italy, 13-16 June 2000.

Berzins, V., "Static Analysis for Program Generation Templates," 7th Monterey Workshop: Modeling Software System Structures in a Fast Moving Scenario, Santa Margherita Ligure, Italy, 13-16 June 2000.

Chaki, N., "High Level Net Models: A Tool for Fault-Detection in Multi-stage Interconnection Network," IEEE Region 10 Conference (TENCON) 2000, Kuala Lumpur, Malaysia, 24-27 September 2000.

Bhattacharya, S., "Automated Generation of Wrappers for Interoperability," 2000 Command and Control Research and Technology Symposium, Monterey, CA, 26-28 June 2000.

Ge, J., "Computer Aided Prototyping in a Distributed Environment," International Congress on Intelligent Systems and Applications (ISA2000), Australia, 12-15 December 2000.

Zhang, D., "A Framework for Natural Language Agents," Ninth International Conference on Intelligent Systems, Louisville, KY, June 2000.

Kiselyov, O., "Implementing Metcast in Scheme," Workshop on Scheme and Functional Programming, Montréal, Canada, September 2000.

Shing, M., "Computer Aided Prototyping System (CAPS) for Heterogeneous Systems Development and Integration," 2000 Command and Control Research and Technology Symposium, Monterey, CA, 26-28 June 2000.

Luqi, "A Risk Assessment Model for Evolutionary Software Projects," 7th Monterey Workshop: Modeling Software System Structures in a Fast Moving Scenario, Santa Marguerite Figure, Italy, 13-16 June 2000.

Berzins, V., "Prototyping Tool-Kit (APT)," 2nd International Symposium on Constructing Software Engineering Tools (CoSET 2000), ICSE 2000, Limerick, Ireland, 4-11 June 2000.

Schneidewind, N., "Cost Framework for COTS Evaluation," COMPSAC 99, Phoenix, AZ, 27 October 1999.

Schneidewind, N., "Predicting Deviations in Software Quality By Using Relative Critical Value Deviation Metrics," 10th International Symposium on Software Reliability Engineering, Boca Raton, FL, 1-4 November 1999.

Schneidewind, N., "Investigation of the Risk to Software Reliability of Requirements Changes," 1999 NASA Workshop on Risk Management, Morgantown, WV, 28-29 October 1999.

Schneidewind, N., "The Ruthless Pursuit of the Truth about COTS," North Atlantic Treaty Organization, Commercial Off-the-Shelf Products in Defense Applications, Brussels, Belgium, 3-5 April 2000.

THESES DIRECTED:

Augustine, T., "Naval Architecture Environment: Facilitating JV2010," Masters Thesis, Naval Postgraduate School, December 1999.

Gee, K., "An Architectural Framework for Integrating COTS/GOTS/Legacy Systems," Masters Thesis, Naval Postgraduate School, June 1999.

Nguyen, T., "Commercial-Off-The-Shelf (COTS)/Legacy Systems Integration Architectural Design and Analysis," Masters Thesis, Naval Postgraduate School, September 2000.

Tran, T. and Allen, J., "Interoperability and Security Support for Heterogeneous COTS/GOTS/Legacy Component-Based Architecture," Masters Thesis, Naval Postgraduate School, September 2000.

Cheng, N., "Automated Generation of Wrappers for Interoperability," Masters Thesis, Naval Postgraduate School, June 2000.

DoD KEY TECHNOLOGY AREAS: Computing and Software

KEYWORDS: Engineering Automation, Reliability, Glue and Wrapper Technology, Computer-Aided Decision Support

IMPROVED SOFTWARE TECHNOLOGY FOR THE NEXT GENERATION AIRCRAFT CARRIER

Luqi, Professor Department of Computer Science Sponsor: Naval Sea Systems Command

OBJECTIVE: To improve software technology in areas of concern to NAVSEA and to apply the results to software issues arising in the future aircraft carriers such as CVX.

SUMMARY: This project seeks to assess the potential for improved Naval damage control operations with fewer personal enabled by improved communications and decision support technology.

An evaluation of current video tele-conferencing (VTC) technology is complete. The determination of VTC's role and the added value to damage control on CVX is underway and will require some exploration of the TELETECNET training system planned for installation in CVN-75 this fiscal year to consider the asbuilt configuration, limiting factors and training applicability of VTC to carriers.

Evaluation of barcode technology has reached the product identification stage and for lack of materials, may not be adequately considered in this study. A review of the Smart Ship program has been partially completed. Literature reviews and interviews with crew and design personnel have provided a wealth of information. Migration of some Smart Ship technologies into CVX is expected. Some technologies added to Smart Ship have been in place on carriers for several years, including Hydra radio systems. This technology group and the subsequent reductions in manpower achieved suggest that many of the same lessons will be of great value to CVX. A visit to USS YORKTOWN or USS THOMAS S. GATES to examine the 61 technology items in play would benefit this study.

Wireless LAN technology has been studied and evaluated at the present state of the art. Vigorous product development activity in the wireless community suggests that this technology may yield acceptable advancements that will improve the reliability to support shipboard use for damage control. Live onboard testing is vital to the proof of this concept.

Evaluation of an expert system using a simple inference engine has been completed and indicates this outstanding technology should be organic to the damage control communication system. Further testing and development is needed. More robust applications and prototypes are needed to explore beyond the simple demonstration version. Frank Steinbach made a site visit to the CVX Project Office in Crystal City to discuss the tenets of his M.S. thesis; future career plans with regard to CVX and to gain familiarity with the facility there. In the process of the visit, contact was established with Smart Ship personnel PNC John Bealmear (USN Ret) and Ray O'Toole to obtain firsthand accounts of the Smart Ship learning process and to discuss possible avenues of exploration for use for future CVX use.

A small wireless LAN has been constructed to evaluate the viability of signals between computers utilizing COTS hardware and software to gain a working knowledge of the limitations and capabilities of current technology. The most striking weakness in Wireless LAN technology found is the low propagation of signals when mobile units go beyond the line of sight. However, current "leaky cable" techniques employed in internal communications aboard ship may help to mitigate that weakness and support mobile Repair Lockers.

We have performed live set up and testing on three forms of video tele-conferencing to support tele-training for CVX damage control requirements. One form (CNET's Electronic Schoolhouse) of this training is currently in use aboard several fleet units but requires great bandwidth and dedicated facilities. We have set up and operated the NPS distance learning system to ascertain the capabilities of this technology and current protocol standards. Two other forms, "Video on Demand" (VOD) and desktop teleconferencing, allow users on general computer assets throughout a ship to participate in training without leaving their own work area. Our test of Precept Corporation's "IPTV" demonstrated that Damage Control training could be conducted through desktop computers throughout a ship via the LAN without the requirement to "Stack" bandwidth for each user. This bodes well for the ability to accomplish multiple

channels or topics of study at the same time. Several student theses have been reviewed to develop a fuller understanding of Video Technology.

We have constructed a small model of an expert system to demonstrate the ability to program a logical sequence of routines into a simple program on a PC. This technology, if extended, will allow Damage Control Locker Leaders and the Damage Control Assistant to evaluate him/herself in a training situation or to sanity check decisions in a hot environment when lives are at risk while deciding on actions to combat fires, flooding and contamination. This technology is not yet being used to our knowledge but was explored here at NPS in the 1980's when GUI interfaces and rapid prototyping CASE tools were not available. Our contention is that this technology has matured to the point of deserving another hard look. We have acquired a copy of a 1996 study conducted by David Tate at the Naval Research Labs. Tate concludes that decision aids based on inference engines are vital to the effective control of manpower and resources in a tactical damage control situation. We have put up a small web page of technology sources that have contributed to the knowledge collected thus far in our research.

PUBLICATION:

CIDE Supporting Technology and Infrastructure, Final Report.

THESIS DIRECTED:

Williamson, C., "A Sharp Evolution: Development of the Sierra Hotel Aviation Reporting Program from the Deck Plates," Masters Thesis, Naval Postgraduate School, September 2000.

DoD KEY TECHNOLOGY AREAS: Computing and Software, Command, Control and Communications

KEYWORDS: Interoperability, C4ISR, Combat Systems, CVX

COMPUTER SUPPORT FOR POLICY

James Bret Michael, Associate Professor
Department of Computer Science
Sponsor: Naval Postgraduate School Research Initiation Program

OBJECTIVE: To explore both the architecture for and components of a computer-based intelligent assistant, known as a policy workbench, for partially automating the generation of policy-governed systems.

SUMMARY: A policy workbench is an integrated suite of computer-based tools for representing policy, reasoning about policy, maintaining policy, and embedding policy as procedures (i.e., computer interpretable or executable code) in information systems. A policy is a statement of a goal, doctrine, or rule of an organization. The workbench serves as an intelligent assistant for developing and maintaining policy-governed systems; the workbench assists users and developers of such systems to identify and resolve gaps in policy before high-level requirements and other system artifacts are derived from the policy base. The policy workbench is also intended for use with legacy systems, in addition to constructing composite systems (e.g., systems supporting coalition forces) from extant systems.

We explored the technical feasibility of implementing three of the components of the policy workbench, one of these being an automatic test-case generator. The second component automatically translates natural language statements of policy into a common information model from which computer-based tools can extract policy objects and relationships to generate tool-specific computational representations of policy for further processing. The third component, an integrated policy compiler and tester, were developed and experiments were conducted to determine to what extent policy regarding network management, specified in the Path-based network Policy Language (PPL), could be tested for logical consistency.

In addition to PPL, we explored to what extent the Reference Model for Open-Distributed Processing (RM-ODP) can be used to model policy for distributed systems. We found that identifying inconsistency in policy regarding interoperability of the subsystems of the Ballistic Missile Defense (BMD) system

necessitated the use of multiple viewpoints. Further, we found that firm conclusions about the existence of gaps in the policy base must be deferred until the high-level viewpoints are refined.

We also investigated the potential uses of the workbench to define, measure, specify, and compute trust in the context of distributed systems. We developed a modeling framework for specifying discretionary and mandatory policy about what types of trust-relationships can be created, modified, and destroyed between members of an organization, within sub-organizations, and across organizational boundaries. We investigated how the framework could be used to support the development of both the architecture and requirements for the US DoD's information infrastructure (DII), in addition to local infrastructures (e.g., infrastructures for carrier battle groups and the Navy/Marine Corps Intranet).

PUBLICATION:

Gaines, L.T. and Michael, J.B., "Trust Management in OLAP Tools," *Proceedings of the IFIP WG11.3 Working Conference on Database Security*, Schoorl, The Netherlands, 21-23 August 2000.

THESES DIRECTED:

Gaines, L.T., "Trust and its Ramifications for the DoD Public Key Infrastructure," Masters Thesis, Naval Postgraduate School, September 2000.

Smith, S.A., "The Application of a Viewpoints Framework in the Development of C4I Systems," Masters Thesis, Naval Postgraduate School, June 2000.

Stone, G.N., "A Path-Based Network Policy Language," Ph.D. Dissertation, Naval Postgraduate School, September 2000.

DoD KEY TECHNOLOGY AREAS: Computing and Software

KEYWORDS: Policy, Intelligent Assistant, Distributed Systems, Trust

COGNITIVE MODELING FOR TRAINING

Barry Peterson, Research Assistant Rudy Darken, Assistant Professor Department of Computer Science

Sponsor: Naval Air Warfare Center-Training Systems Division

OBJECTIVE: The virtual environments for training technology (VETT) program and the Modeling, Virtual Environments and Simulation Academic Group will collaborate to identify a new approach to the human cognitive modeling process that will support our common research objectives and the training of individuals in virtual environments.

DoD KEY TECHNOLOGY AREAS: Computing and Software

KEYWORDS: Cognitive Modeling, Virtual Environments, Training

AUTOMATIC UPDATING OF TERRAIN DATABASES FROM SATELLITE IMAGERY

Neil C. Rowe, Associate Professor Department of Computer Science Sponsor: Naval Engineering Logistics Office

OBJECTIVE: We will develop a prototype system to update terrain databases with new features observed in aerial photographs using image differencing.

SUMMARY: In 2000 the first phase of the project was concluded by preparing a journal paper that was accepted in December. The main product is a program that takes two crudely registered aerial photographs, finds the exact registration using line segments, calculates the line segments that do not match, and displays them overlaid on the original images. Efficiency improvements made in January now allow the program to provide results in 8 minutes for 256 by 256 image pairs where it previously took 90 minutes.

PUBLICATIONS:

Rowe, N.C. and Alexander, R.S., "Finding Optimal-Path Maps for Path Planning Across Weighted Regions," *International Journal of Robotics Research*, 2 February 2000, pp. 83-95.

Rowe, N.C., Grewe, L., and Baer, W., "A Digital Library of Aerial Photographs Supporting Change Analysis," Poster and presentation at ACM Digital Libraries 2000, San Antonio, TX, June 2000.

PRESENTATIONS:

Hunter, G.K. and Rowe, N.C., "Software Designs for a Fault-Tolerant Communications Satellite," Command and Control Research and Technology Symposium, Monterey, CA, June 2000.

Grewe, L., Rowe, N., and Baer, W., "AERICOMP: An Aerial Photo Comparison System," SPIE Signal Processing, Sensor Fusion, and Target Recognition IX Conference, June 2000.

THESES DIRECTED:

Herman, J., "Target Identification Algorithm for the AN/AAS-44V Forward-Looking Infrared (FLIR)," Masters Thesis, Naval Postgraduate School, June 2000.

Lisowski, M., "Development of a Target Recognition System Using Formal and Semiformal Methods," Masters Thesis, Naval Postgraduate School, December 2000.

DoD KEY TECHNOLOGY AREAS: Computing and Software, Human Systems Interface

KEYWORDS: Images, Captions, Digital Libraries, Information Filtering, Content Analysis

AN OBJECT-ORIENTED DISTRIBUTED ARCHITECTURE FOR THE CAMPEX SOFTWARE

Man-Tak Shing, Associate Professor Department of Computer Science Sponsor: U. S. Army TRADOC Analysis Command

OBJECTIVE: To develop a prototype of an object-oriented distributed architecture for the CAMPEX software.

SUMMARY: The U.S. Air War College uses a set of stand alone war-gaming software, called the Campaign Planning Exercise (CAMPEX), to teach and test its students' understanding of strategy, leadership, international security, National Security Decision Memoranda (NSDM), General Purpose (GP) forces, unified commands, and joint fundamentals in the area of the Air Campaign Planning and the

Ground Forces Deployment. The CAMPEX software was written in the Basic programming language. Its life cycle started in 1986 and the last version was released in 1994. There is a need to modernize CAMPEX into a Web-based application to take advantage of modern Personal Computers and the World Wide Web. The research conducted in this project succeeded in re-engineering CAMPEX into a web-based platform independent system executable on any networked computer. The research effort produced a set of requirements and an object-oriented design for the enhanced Web-based simulation. The correctness of requirements has been validated via a prototype developed using ACCESS 2000. The new design will be the basis for reengineering the other war game planning software for the Air War College.

PUBLICATION:

Shing, M., Jackson, L., and Chalakatevakis, A., "Architectural Design and Prototyping of a Web-Based War Game Simulation For Campaign Planning Exercises," to appear in the *Proceedings of the 13th Annual Software Engineering Conference*, Salt Lake City, UT, 29 April-4 May 2001.

PRESENTATION:

Shing, M., Jackson, L., and Chalakatevakis, A., "Architectural Design and Prototyping of a Web-Based War Game Simulation For Campaign Planning Exercises," 13th Annual Software Engineering Conference, Salt Lake City, UT, 29 April-4 May 2001.

THESIS DIRECTED:

Chalakatevakis, A., "Architectural Design and Prototyping of a Web-Based War Game Simulation for Campaign Planning Exercises," Masters Thesis, Naval Postgraduate School, September 2000.

DoD KEY TECHNOLOGY AREAS: Battlespace Environments, Computing and Software, Modeling and Simulation

KEYWORDS: Battlespace Environments, Distributed Components Architecture, Object-Oriented Design, Modeling and Simulation.

TYPE SYSTEMS FOR SECURE REMOTE EVALUATION

Dennis Volpano, Associate Professor Department of Computer Science Sponsor: National Science Foundation

OBJECTIVE: This is a joint project with Geoffrey Smith at the Florida International University (FIU). The work is part of a continuing project aimed at investigating the role of programming language design and type systems in ensuring the privacy of data in programs. The long-term objective is to identify how languages should be designed in order to be able to prove confinement properties about programs expressed in them. This is the final year of the project.

SUMMARY: In previous years of the project we developed various flavors of Noninterference to capture confinement in different kinds of programming languages. We started with a simple imperative, deterministic language, then looked at a nondeterministic one, and finally a probabilistic one. Confinement is captured by three different Noninterference properties, respectively, NI, Possibilistic NI, and Probabilistic NI. In the final year of the project, we formally characterized the difference between safety properties and confinement properties.

Each however is too strong to allow practical primitives. For example, in password-based authentication, anyone can enter a password and find out whether it is correct. This would be disallowed in any system satisfying NI. To justify a system of this kind, we turned to computational complexity. Investigation continued into probabilistic timing channels and techniques for eliminating them in

concurrent programs. Secrecy was also contrasted formally with safety properties. It was shown that secrecy relates the traces of a program's execution whereas safety does not.

DoD KEY TECHNOLOGY AREAS: Computing and Software

KEYWORDS: Programming Language Design

BASIC RESEARCH IN INFORMATION PRIVACY

Dennis Volpano, Associate Professor
Department of Computer Science
Sponsor: National Science Foundation and Naval Postgraduate School

OBJECTIVE: This is a joint project with Geoffrey Smith at the Florida International University (FIU). The work is part of a continuing project aimed at investigating new techniques for proving privacy in systems that downgrade information, for instance, through use of cryptography. New relative notions of secrecy are needed that relate the complexity of leaking secrets in systems to that of breaking cryptographic primitives. Simple examples include password systems that store passwords as images under a one-way function.

SUMMARY: In our previous work, it was proven that leaking a secret S in a deterministic program is as hard as deducing S using only match queries of the form "Does S = Y, for a given string Y?" It can be proved that there is no polynomial time algorithm for deducing a k-bit integer secret S, for all k, if the algorithm is limited to accessing S via these queries.

And, further, no polynomial time algorithm can do it with non-negligible probability if secrets are uniformly distributed and of sufficient size.

Next we considered a one-way hash function H that is characterized by collision resistance. Given H (z), find an x such that H (x)=H (z). Hash functions are not allowed in any system that satisfies NI. Sets of conditions were given under which a one-way hash function can be used safely in programs. It was proved that the existence of an efficient

Deterministic algorithm that meets the conditions and deduces the value of a high input variable v, given H (v), implies there is an efficient probabilistic algorithm for inverting H.

DoD KEY TECHNOLOGY AREAS: Computing and Software

KEYWORDS: Programming Languages, Security, Privacy

NETWORK MANAGEMENT SYSTEMS FOR INTEGRATED SERVICES, SAAM

Geoffrey G. Xie, Assistant Professor
Department of Computer Science
Sponsor: Defense Advanced Research Projects Agency

OBJECTIVE: We are developing a novel server and agent based active management system for the next generation Internet.

SUMMARY: We made progress in the following areas:

(1) Self-repairing Signaling Channels: A Key requirement for SAAM is the ability to reconfigure the signaling channels automatically and in near real time to accommodate changes in network topology. We developed a pro-active approach that refreshes SAAM signaling channels over short time intervals in anticipation of topological changes. The overhead of the resulting protocol is very manageable. On average, each router needs to process two control messages in each refresh cycle. The protocol also provides a means for each router to periodically report its link state information to the server without imposing additional processing overhead on the intermediate routers.

- (2) Intelligent Resource Manager: We focused on optimality rather than complexity in designing the resource manager to run on a SAAM server. The resulting system supports all service classes defined by major Internet service models (Integrated Services, Differentiated Services, and Multi-Protocol Label Switching) in a cohesive manner. It maintains a comprehensive path information base to aid QoS routing and rerouting and optimizes the utilization of network resources via adaptive routing and dynamic link provisioning between service classes.
- (3) Server Fault Tolerance: We investigated how to make SAAM services tolerant of server failures. There are two types of server failures. Most are transient and recoverable like component failures. The others are catastrophic failures, not recoverable in a short time. For the first type, we examined current commercial offerings and concluded that several of these might be suitable for SAAM. The second type of failures can best be dealt with by using a backup server. No commercial product meets the stringent requirement of SAAM service availability. We developed a protocol that can detect server failure and resume full service within fractions of a second. The backup server uses adaptive polling, with the cycle time becoming persistently smaller with each unanswered probe, to detect and verify primary server failure in a timely and reliable manner.
- (4) System Security: Security is particularly important for SAAM because SAAM uses mobile code, called resident agents, to extend router services. The server loads these resident agents onto routers dynamically, and the agents then execute on the destination routers. A scheme to authenticate mobile code is required to prevent an outsider from installing a malicious resident agent. Also, all signaling messages in SAAM are authenticated to counter spoofing attacks. We explored the idea of Time-driven Key Sequencing (TKS) to speed up the authentication process. TKS is a scheme for implementing low-overhead key changes in support of the use of efficient cryptographic algorithms. We also developed a Kerberos-based method to authenticate new nodes that join a SAAM network and to refresh authentication keys across the network.
- (5) Server Originated Probing: The objective of this work is to add server-based, router performance sampling capabilities to SAAM. As a router may be misconfigured, or worse, actively attacked, a server should not rely entirely on link performance data reported by routers to maintain the network status. We developed a method that gives the server an independent means to validate link performance reports from a router. This way, erroneous performance data can be filtered out before it causes severe service degradation.
- (6) Path-based network Policy Language (PPL): Existing network policy languages define policy rules on a per node basis. PPL's path-based approach for representing network policies is advantageous in that QoS and security policies can be associated with an explicit path through the network. This assignment of policies to network flows aids in new initiatives such as Integrated Services. The more stringent requirement of supporting path-based policies can be easily relaxed with the use of wild card characters to also support Differentiated Services and best-effort service. Path-based policies have a complexity advantage over node-based ones as well.
- (7) Configuration Management: We formalized and simplified SAAM testbed configuration management. We defined a SAAM configuration language using XML and developed a GUI based application to help users create test configurations in the defined language. The demo-station was also modified accordingly; it now sets up a SAAM testbed by reading a test configuration file.

PUBLICATIONS:

Xie, G.G., Irvine, C., and Levin, T., "Conditions for Time-driven Key Sequencing," Naval Postgraduate School Technical Report, August 2000. (An enhanced version submitted to Usenix Security Conference.)

Xie, G.G. and Gibson, J. A., "Networking Protocol for Underwater Acoustic Networks," Naval Postgraduate School Technical Report, December 2000.

PRESENTATIONS:

Xie, G.G., "Signaling, Security, and A Policy Language for SAAM," DARPA Next Generation Internet PI Meeting, McLean, VA, October 2000.

Xie, G.G., "The Next Generation Internet," MOVES Open House, Monterey, CA, August 2000.

THESES ADVISED:

Stone, G., "A Path Based Policy Language," Ph.D. Dissertation, Naval Postgraduate School, September 2000.

Gibson, J. and Kuo, D.C., "Design of a Dynamic Management Capability for the Server and Agent Based Active Network Management (SAAM) System," Masters Thesis, Naval Postgraduate School, September 2000.

Ababneh, M., "Network Configuration Using XML," Masters Thesis, Naval Postgraduate School, September 2000.

Velazques, L. and Szczepankiewicz, P., "Authentication in SAAM Routers," Masters Thesis, Naval Postgraduate School, June 2000.

Akkoc, H., "A Pro-Active Protocol for Configuration of Signaling Channels in Server and Agent-based Active Network Management (SAAM)," Masters Thesis, Naval Postgraduate School, June 2000.

Uysal, H.H., "A Model for Generation and Processing of Link State Information in SAAM Architecture," Masters Thesis, Naval Postgraduate School, March 2000.

Kati, E., "Fault Tolerant Approach for Development of SAAM Server in Windows NT Environment to Provide Uninterrupted Services to Routers," Masters Thesis, Naval Postgraduate School, March 2000.

Quek, H.C., "QoS Management with Adaptive Routing for Next Generation Internet," Masters Thesis, Naval Postgraduate School, March 2000.

Altinkaya, M., "Server Probing for Server and Agent Based Active Network Management," Masters Thesis, Naval Postgraduate School, March 2000.

DoD KEY TECHNOLOGY AREAS: Computing and Software, Command, Control and Communications

KEYWORDS: Network Management, Integrated Services, Asynchronous Transfer Mode (ATM), Quality of Service (QoS), Policy Based Networking, Network Security